

**RECEIVED
CENTRAL FAX CENTER**

JAN 23 2008

CLAIM AMENDMENTS**Please amend the claims as indicated below:**

1.(Currently amended) A method for biometrically securing access to a user-desired activity, said method comprising the steps of:

establishing a contactless communication link between a portable electronic device associated with a user and an electronic system associated with a user-desired activity;

~~wirelessly obtaining an identification including biometric attributes of a user using an through said electronic system associated with a user-desired activity and adapted for supporting wireless communication with from said portable electronic devices the identification of said user further retrieved from a portable electronic device associated with said user after said portable electronic device establishes a contactless communication link to support wireless communication between said portable electronic device and said electronic system;~~

accessing a user profile including biometric attributes associated with said user by said electronic system associated with a user-desired activity through a computer network from a remote server based on the identification including ~~biometric attributes of said user obtained~~ wirelessly by said electronic system from said portable electronic device ~~contactless smart card;~~

~~comparing said identification including biometric attributes obtained wirelessly by said electronic system from said portable electronic device with said user profile including biometric attributes obtained by said electronic system from said remote server to determine if biometric attributes from said portable electronic device match biometric attributes from said server;~~

~~if biometric attributes from said contactless smart card match biometric attributes from said server, prompting said user to input to a biometric user interface associated with said electronic system~~ associated with a user-desired activity ~~at least one biometric attribute randomly selected from biometric attributes accessed by said electronic system from at least one of said remote server and said portable electronic device; and~~

permitting said user to perform a user-desired activity if at least one biometric attribute input by said user to said biometric user interface associated with said electronic system matches at least one biometric attribute randomly selected by said electronic system associated with a user-desired activity from biometric attributes accessed by said electronic system associated with a user-desired activity from ~~at least one of said~~ said user profile including

biometric attributes associated with said user through said computer network from said remote server and said portable electronic device.

2.(Previously presented) The method of claim 1 wherein said computer network is a secure computer network.

3.(Previously amended) The method of claim 1 wherein said remote server is a biometric broker.

4.(Previously amended) The method of claim 1 wherein said portable electronic device is at least one of: a smart card, PDA, cellular telephone.

5.(Original) The method of claim 4 further comprising the step of:
permitting said user to modify said user profile, in response to approval of a request by said user.

6.(Cancelled).

7.(Previously amended) The method of claim 1 further comprising the step of:
subsequently prompting a user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile, if at least one biometric attribute previously input by said user to said biometric user interface associated with said electronic system does not match said at least one biometric attribute previously randomly selected.

8.(Original) The method of claim 1 wherein said electronic system comprises at least one wireless device that operates with a wireless network.

9.(Original) The method of claim 1 wherein said electronic system comprises at least one computer workstation operable over an associated network.

10.(Original) The method of claim 1 wherein said electronic system comprises an automated teller machine.

11.(Previously amended) The method of claim 1 wherein said electronic system comprises a secured entry.

12.(Original) The method of claim 1 wherein said electronic system comprises a wireless network.

13.(Cancelled)

14.(Original) The method of claim 1 wherein said electronic system comprises a wireless device.

15.(Previously presented) The method of claim 1 further comprising the steps of:

identifying at least one defective biometric attribute associated with said user; and thereafter prompting a user to input to said biometric user interface associated with said electronic system at least one additional biometric attribute randomly selected from said user profile containing biometric attributes of said user.

16.(Original) The method of claim 1 wherein said user-desired activity comprises a financial transaction.

17.(Original) The method of claim 1 wherein said user-desired activity comprises an ATM transaction.

18.(Original) The method of claim 1 wherein said user-desired activity comprises access to a secure area.

19.(Original) The method of claim 1 wherein said user-desired activity comprises access to data from said electronic system.

20.(Original) The method of claim 1 wherein said user-desired activity comprises execution of a mechanical activity.

21.(Original) The method of claim 1 further comprising the step of:

initiating access to said electronic system utilizing only one biometric attribute input to said electronic system.

22.(Currently amended) A method for biometrically securing access to a secure area, said method comprising the steps of:

wirelessly obtaining an identification ~~including biometric attributes~~ of a user from a contactless smart card by an electronic system using a contactless card reader in communication with said electronic system; ~~the identification including biometric attributes of said user further retrieved from said contactless smart card after said contactless smart card establishes a contactless link with said contactless card reader that supports wireless communication between said contactless smart card and said contactless card reader;~~

said electronic system using a computer network to obtain a user profile including ~~biometric attributes~~ associated with said user from a remote server based on said identification;

~~comparing said identification including biometric attributes obtained wirelessly by said electronic system from said contactless smart card with said user profile including biometric attributes obtained by said electronic system from said remote server to determine if biometric attributes from said contactless smart card match biometric attributes from said server;~~

~~if biometric attributes from said contactless smart card match biometric attributes from said server,~~ said electronic system prompting said user to input into a biometric user interface associated with said electronic system at least one biometric attribute randomly selected by said electronic system from biometric attributes accessed by said electronic system from at least one of said remote server ~~and said contactless smart card~~; and

permitting said user to access a secure area if at least one biometric attribute input by said user to said biometric user interface matches at least one biometric attribute randomly selected by said electronic system from biometric attributes accessed by said electronic system.

23.(Currently amended) A system for biometrically securing access to a user-desired activity, said system comprising:

a biometric user interface; and

an electronic system adapted to i) wireless communicate with portable electronic devices, ii) communicate with remote servers, iii) ~~compare~~ obtain user identification ~~including biometric attributes obtained wirelessly by said electronic system from a portable electronic device with~~ to obtain a user profile including biometric attributes ~~obtained by said electronic system from a remote server to determine if biometric attributes obtained from said contactless smart card match biometric attributes obtained from said server,~~ iv) receive biometric attributes from a user through said biometric user interface associated with said electronic system, and v) permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches at least one biometric attribute randomly selected by said electronic system from ~~at least one of: a user profile including biometric attributes associated with said user accessible by the electronic system from a remote server or an identification including biometric attributes associated with said user obtained wirelessly from a portable electronic device in wireless communication with the electronic system, if said electronic system determines that biometric attributes associated with said user obtained from said remote server match biometric attributes associated with said user obtained from said portable electronic device.~~

24.(Cancelled).

25.(Previously amended) The system of claim 23 wherein said user profile including biometric attributes is accessible from a biometric broker via a secure network connection.

26.(Previously amended) The system of claim 23 wherein said remote server is a biometric broker.

27.(Previously amended) The system of claim 23 wherein said biometric user interface is adapted to accept at least one of the following attributes from a user: fingerprint, iris, voice, signature, facial, hand geometry, retinal, palm, ear DNA, keystroke, body odor.

28.(Cancelled).

29.(Cancelled).

30.(Original) The system of claim 23 wherein said electronic system comprises at least one wireless device that operates with a wireless network.

31.(Previously submitted) The system of claim 23 wherein said electronic system comprises at least one computer workstation accessible over said computer network.

32.(Previously amended) The system of claim 23 wherein said electronic system comprises an automatic_teller machine.

33.(Original) The system of claim 23 wherein said electronic system comprises a secured entry system to a secured environment.

34.(Previously amended) The system of claim 23 wherein said computer network comprises a wireless network.

35.(Cancelled).

36.(Previously amended) The system of claim 23 wherein said portable electronic device comprises at least one of a wireless device, a contactless smart card, a PDA, a cellular phone.

37.(Previously amended) The system of claim 23 further comprising:

module for identifying at least one defective biometric attribute associated with said user; and

wherein said system is adapted by said module whereby said_user is thereafter prompted to input to said electronic system at least one additional biometric attribute randomly selected from a user profile containing biometric attributes of said user.

38.(Original) The system of claim 23 wherein said user-desired activity comprises a financial

transaction.

39.(Original) The system of claim 23 wherein said user-desired activity comprises an ATM transaction.

40.(Original) The system of claim 23 wherein said user-desired activity comprises access to a secure area.

41.(Original) The system of claim 23 wherein said user-desired activity comprises access to data from said electronic system.

42.(Original) The system of claim 23 wherein said user-desired activity comprises execution of a mechanical activity.

43. (Original) The system of claim 23 wherein access to said electronic system is initiated utilizing only one biometric attribute input to said electronic system.

44.(Cancelled).

45. (Currently amended) A system for biometrically securing access to a user-desired activity, said system comprising:

a biometric user interface electronically associated with an electronic system adapted to:

receive biometric attributes from a user through said biometric user interface;

an electronic system adapted to:

wirelessly communicate with contactless smart cards;

communicate with remote servers;

~~compare obtain user identification including biometric attributes obtained~~
wirelessly by said electronic system from a contactless smart card with for use to obtain

a user profile including biometric attributes ~~obtained by said electronic system from a remote server to determine if biometric attributes obtained from said contactless smart card match biometric attributes obtained from said server;~~

~~receive biometric attributes from a user through said biometric user interface;~~
and

permit a user to perform a user-desired activity if at least one biometric attribute input by the user to said biometric user interface matches at least one biometric attribute randomly selected by said electronic system from ~~at least one of~~ a user profile including biometric attributes associated with said user accessible by the electronic system from a remote server and based on identification including ~~biometric attributes associated with~~ of said user obtained wirelessly from a contactless smart card ~~in wireless communication with a contactless card reader associated with the electronic system if said electronic system determines that biometric attributes associated with said user obtained from said remote server match biometric attributes associated with said user obtained from said contactless smart card.~~